I. REAL PARTY IN INTEREST 1

II. RELATED APPEALS AND INTERFERENCES 2

III. STATUS OF CLAIMS 2

IV. STATUS OF AMENDMENTS 2

V. SUMMARY OF CLAIMED SUBJECT MATTER 2

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL 4

VII. THE ARGUMENT 4

VIII. CLAIMS APPENDIX 13

IX. EVIDENCE APPENDIX 17

X. RELATED PROCEEDINGS APPENDIX 18

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number:	10/789,574
Filing Date:	2/27/2004
Applicant(s):	Matthew P. Chant et al.
Entitled:	CLASSIFYING E-MAIL CONNECTIONS FOR POLICY ENFORCEMENT
Examiner:	Jungwon Chang
Group Art Unit:	2154
Attorney Docket No.:	LOT920040002US1 (7321-044U)

TRANSMITTAL OF APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Submitted herewith is Appellant's Appeal Brief in support of the Notice of Appeal filed July 17, 2008. As this Appeal Brief has been timely filed within the shortened statutory period of two months from the date of the Notice of Appeal, no extension of time under 37 C.F.R. § 1.136 is required. Notwithstanding, please charge any shortage in fees due under 37 C.F.R. §§ 1.17, 41.20, and in connection with the filing of this paper, including extension of time fees, to Deposit Account 12-2158, and please credit any excess fees to such deposit account.

Date: September 17, 2008

Respectfully submitted,

/Steven M. Greenberg/
Steven M. Greenberg, Registration No. 44,725
Customer Number 46321

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number:	10/789,574
Filing Date:	2/27/2004
Applicant(s):	Matthew P. Chant et al.
Entitled:	CLASSIFYING E-MAIL CONNECTIONS FOR POLICY ENFORCEMENT
Examiner:	Jungwon Chang
Group Art Unit:	2154
Attorney Docket No.:	LOT920040002US1 (7321-044U)

APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This Appeal Brief is submitted in support of the Notice of Appeal filed July 17, 2008, wherein Appellants appeal from the Examiner's rejection of claims 1 through 20.

I. REAL PARTY IN INTEREST

This application is assigned to International Business Machines Corporation by assignment recorded on February 27, 2004, at Reel 015038, Frame 0553.

II. RELATED APPEALS AND INTERFERENCES

Appellant is unaware of any related appeals and interferences.

III. STATUS OF CLAIMS

Claims 1 through 20 are pending in this Application and have been twice rejected. It is from the multiple rejections of claims 1 through 20 that this Appeal is taken.

IV. STATUS OF AMENDMENTS

Claims 1, 4, 12 and 15 were amended in an amendment dated January 28, 2008 (the "Amendment").

V. SUMMARY OF CLAIMED SUBJECT MATTER

By reference to paragraph [0015] of Appellants' published specification, Appellants have invented a system, method and apparatus for classifying and processing process incoming electronic mail messages based upon associated policies. In accordance with Appellants' invention, prior to delivering an electronic message to a mail client, the incoming electronic message can be classified based upon the source of the incoming message. A policy associated with the classification can be used to determine how to process the incoming message. For instance, at one extreme a policy can indicate that all messages associated with a trusted classification are to be delivered, while at another extreme, a policy can indicate that all messages associated with a blocked classification are never to be delivered. In this way, spam

can be intelligently handled uniformly and automatically without regard to the varying nature of disparate electronic mail clients.

With specific reference to claim 1, a method for classifying electronic mail message transfer requests for policy enforcement is provided. (Par. [0019]) The method includes identifying a source of an incoming electronic message, (Par. [0019]) classifying the source, (Par. [0020]) selecting a message transfer policy based upon the classification, (Par. [0022]) and applying the selected message transfer policy to the incoming electronic message. (Par. [0022])

With specific reference to claim 10, a system for classifying electronic mail message transfer requests for policy enforcement is provided. (Par. [0016]) The system includes a mail server (Par. [0016]) and a set of mail transfer policies, (Par. [0018]) each policy having an association with a corresponding source classification. (Par. [0018]) The system also includes at least one table of source identities having a particular classification (Par. [0017]) and a classifier coupled to the mail server and the table. (Par. [0017]) The classifier identifies a source of an incoming electronic message in the mail server, (Par. [0018]) classifies the source with a classification in the table, (Par. [0018]) selects one of the mail transfer policies based upon the classification, and applies the selected one of the mail transfer policies to the incoming electronic message. (Par. [0018])

With specific reference to claim 12, a machine readable storage is provided to have stored thereon a computer program for classifying electronic mail message transfer requests for policy enforcement. (Par. [0024]) The computer program includes a routine set of instructions

(Par. [0025]) which when executed by a machine cause the machine to perform operations including identifying a source of an incoming electronic message, (Par. [0019]) classifying the source, (Par. [0020]) selecting a message transfer policy based upon the classification, (Par. [0022]) and applying the selected message transfer policy to the incoming electronic message. (Par. [0022])

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1 through 9 and 12 through 20 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over United States Patent No. 7,206,814 to Kirsch in view of U.S. Patent No. 7,127,741 to Bandini et al. (Bandini).

Claims 10 and 11 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over United States Patent No. 7,224,778 to Aoki in view of Bandini.

VII. THE ARGUMENT

THE REJECTION OF CLAIMS 1 THROUGH 9 AND 12 THROUGH 20 UNDER 35 U.S.C. § 103

For convenience of the Honorable Board in addressing the rejections, claims 2 through 9 stand or fall together with claim 1 and claims 13 through 20 stand or fall together with claim 12.

In rejecting claims under 35 U.S.C. § 103, it is incumbent upon the Examiner to establish a factual basis to support the legal conclusion of obviousness.[1] In so

[1] See In re Fine, 837 F.2d 1071, 1073 (Fed. Cir. 1988).

doing the Examiner must make the factual determinations set forth in Graham v. John Deere Co.[2] Thereafter, the Examiner bears the initial burden, on review of the prior art or on any other ground, of presenting a prima facie case of unpatentability.[3] Furthermore, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness; however, the analysis need not seek out precise teachings directed to the specific subject matter of the challenged claim, for a court can take account of the inferences and creative steps that a person of ordinary skill in the art would employ.[4]

Of note, obviousness is a legal conclusion based on underlying factual determinations of four general types, all of which must be considered by the trier of fact: (1) the scope and content of the prior art; (2) the level of skill in the art; (3), the differences between the claimed subject matter and the prior art; and (4) any objective indicia of nonobviousness.[5] Applicants' position is that the Examiner has not properly established the underlying facts regarding (1) the scope and content of the prior art and (3) the differences between the claimed invention and the prior art.

Claim 1 recites a method for classifying electronic mail message transfer requests for policy enforcement. For the convenience of the Honorable Board, the entirety of claim 1 is reproduced as amended:

> 1. A method for classifying electronic mail message transfer requests for policy enforcement comprising the steps of:

---

[2] 383 U.S. 1, 17 (1966).

[3] In re Oetiker, 977 F.2d 1443, 1445 (Fed. Cir. 1992).

[4] KSR Int'l Co. v. Teleflex Inc., 127 S. Ct. 1727, 1741 (2007)(quoting In re Kahn, 441 F.3d 977, 988 (Fed. Cir. 2006)).

[5] See KSR Int'l Co. v. Teleflex Inc., 127 S.Ct. 1727, 1734, 82 USPQ2d 1385, 1391 (2007); Graham v. John Deere Co., 383 U.S. 1, 17-18, 148 USPQ 459, 467 (1966); Continental Can Co. USA, Inc. v. Monsanto Co., 948 F.2d 1264, 1270, 20 USPQ2d 1746, 1750-51 (Fed. Cir. 1991); Panduit Corp. v.Dennison Mfg. Co., 810 F.2d 1561, 1566-68, 1 USPQ2d 1593, 1594 (Fed. Cir. 1987).

identifying a source of an incoming electronic message;

classifying said source;

selecting a message transfer policy based upon the classification; and,

applying the selected message transfer policy to said incoming electronic message..

Integral to claim 1 (and also claim 12) is the selection of a message transfer policy based upon a classification of a source of an incoming electronic message and the application of the selected policy to the incoming electronic message.

In the Amendment, Appellants alerted Examiner to the deficiencies of both Kirsch and Aoki for the teaching of "selecting a message transfer policy based upon the classification". Specifically, on page 10 of the Amendment, Appellants stated,

> Indeed, Kirsch shows e-mail filtering through a categorization of received e-mail messages based on information about the sender. However, the process taught in Kirsch is a direct process which is proprietary to the e-mail client. (See e.g. Figure 1, Element 64--the "filtering software"). Likewise, in Aoki, filtering rules are incorporated into the message delivery process and stored in a subscription database accessible to a recipient user. Yet, again, the filtering rules are applied proprietarily by the "mail subscription manager" (See e.g. Figure 1, Element 32--the "mail subscription manager").
>
> Applicants' invention, however, avoids proprietary solutions by reverting to policy driven decision making in order to provide "a more effective methodology for combating spam exclusive of the client side mail client which can span varying mail clients while maintaining a constant level of effectiveness" as set forth in paragraph [0008] of Applicants' specification. In this regard, instead of directly applying rules to inbound messages based upon the identity of a sender of the message, in the Applicants' invention, a policy is selected based upon the identity of the sender, irrespective of the nature of the policy. Thereafter, the policy is applied to the inbound message. Consequently, the underlying policy can change without affecting the underlying selection logic of the e-mail client..

In response, on page 3 of the Final Office Action dated April 17, 2008 (the "Final Office Action"), Examiner argues

> Although Kirsch discloses applying a message transfer policy based upon the classification (fig. 2 shows when the source is classified as a whitelist, **the message transfer policy is applied to send to recipient 104**, when the source is classified as a blacklist, the message transfer policy is applied to process according to recipients instruction's 108, when the source is classified as unsolicited email, the message transfer policy is applied to send to spam folder 116), and it would have been obvious
> that the message transfer policy has to be selected prior to apply the message transfer policy, Kirsch does not specifically disclose selecting a message transfer policy based upon the

classification. Bandini discloses selecting a message transfer policy based upon the classification (figs. 3-4; col. 5, line 14 - col. 6, line 10, ..email is prohibited from being sent, or sources from which email cannot be received ... high priority messages can be passed through immediately"; col. 7, lines 6-33). It would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine the teachings of Kirsch and Bandini because Bandini's selecting a message transfer policy based upon the classification would allow the system to be easily applied the selected policies to users, as taught by Bandini (col. 7, lines 30-33).

At the outset, Appellants note that Examiner has failed to provide a claim construction for the disputed limitation of "message transfer policy" and, in fact, has read the critical limitation "message transfer policy" out of Appellants' claims 1 and 12.

Specifically, on page 3 of the Final Office Action, Examiner refers to Figure 2 of Kirsch and states, "[T]he message transfer policy is applied to process according to recipients instruction's 108". Referring to Figure 2 as reproduced in its entirety,

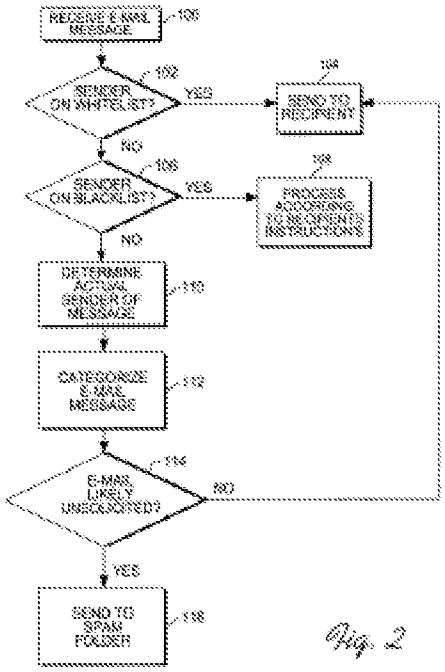

Fig. 2

A sender of a message is classified in block 106 and thereafter, the message is processed according to instructions. Thus, the reference to Figure 2 provides for a jump from classifying a source of a message to processing according to instructions without an intermediate step of selecting a policy to

determine how to process the message as expressly recited in Appellants' claims 1 and 12. Thus, Examiner in failing to provide a relevant claim construction for "message transfer policy" and in fact providing an implied claim construction of no meaning at all has committed clear error as well-understood under the law.[6]

In this regard, "message transfer policy" enjoys a facial meaning of "a definite course or method of action for transferring a message selected from among alternatives and in light of given conditions to guide and determine present and future decisions" as will be confirmed from the plain meaning of policy set forth in many popular dictionaries. Appellants' use of the term "message transfer policy" in paragraph [0015] of Appellants' specification is consistent with the ordinary meaning of "message transfer policy". In this regard, Appellant's state at paragraph [0015],

> A policy associated with the classification can be used **to determine how to process the incoming message**. For instance, at one extreme a policy can indicate that all messages associated with a trusted classification are to be delivered, while at another extreme, a policy can indicate that all messages associated with a blocked classification are never to be delivered. In this way, spam can be intelligently handled uniformly and automatically without regard to the varying nature of disparate electronic mail clients.

Examiner, by comparison, alleges that Figure 2 teaches the presence of a policy without specifying where in Figure 2 such a teaching can be found. Yet, Examiner's very reference to Figure 2 which clearly teaches the classification of a source of a message and the transferring of the message according to the source, implicitly provides for no meaning for the claim term "message transfer policy"--an act by Examiner prohibited under the law in that during patent examination, the pending claims must be "given their broadest reasonable interpretation consistent with the specification."[7] The Federal Circuit's en banc decision in Phillips v. AWH Corp.[8] expressly

---

[6] See Gechter v. Davidson, 116 F.3d 1454, 1460 (Fed. Cir. 1997) (requiring explicit claim construction as to any terms in dispute).
[7] M.P.E.P. 2111.

recognized that the United States Patent and Trademark Office employs the "broadest reasonable interpretation" standard. Examiner's failure to properly construe "message transfer policy" as set forth in claims 1 and 12 obliterates the standard set forth in Phillips and is clear reversible error.

Of course, it goes without saying that Examiner's failure to properly construe or even account for "message transfer policy" does not permit a proper comparison of the cited art to Appellants' claimed subject matter to provide for the identical disclosure of Appellants' claimed subject matter in the cited art as required to establish a prima facie case of obviousness under 35 U.S.C. § 103. Accordingly, there can be found no teaching within Kirsch of "selecting a message transfer policy based upon the classification (of a source of the message)"

Much of the dispute between Examiner and Appellants can be attributed to Examiner's failure to positively map the limitation of "message transfer policy" to a specific portion of Kirsch. The law requires, however, that in rejecting claims for want of novelty or for obviousness, the Examiner must cite the best references at his or her command and when a reference is complex or shows or describes inventions other than that claimed by the applicant, the particular part relied on must be designated as nearly as practicable. The pertinence of each reference, if not apparent, must be clearly explained and each rejected claim specified. The

---

[8] 415 F.3d 1303, 75 USPQ2d 1321 (Fed. Cir. 2005)(The Patent and Trademark Office ("PTO") determines the scope of claims in patent applications not solely on the basis of the claim language, but upon giving claims their broadest reasonable construction "in light of the specification as it would be interpreted by one of ordinary skill in the art." In re Am. Acad. of Sci. Tech. Ctr., 367 F.3d 1359, 1364[, 70 USPQ2d 1827] (Fed. Cir. 2004). Indeed, the rules of the PTO require that application claims must "conform to the invention as set forth in the remainder of the specification and the terms and phrases used in the claims must find clear support or antecedent basis in the description so that the meaning of the terms in the claims may be ascertainable by reference to the description." 37 CFR 1.75(d)(1).)

importance of the specificity requirement of 37 C.F.R. § 1.104(c) is evident in M.P.E.P. § 706.07, which states:

> The examiner should never lose sight of the fact that in every case the applicant is entitled to a full and fair hearing, and that a clear issue between applicant and examiner should be developed, if possible, before appeal.

A clear issue, however, cannot be developed between Appellants and the Examiner where the basis for the Examiner's rejection of the claims is ambiguous. The Examiner's "analysis" provides little insight as to (i) how the Examiner is interpreting the elements of the claims and (ii) what specific features within Kirsch the Examiner believes identically discloses the specific elements (and interactions between elements) recited in the claims--namely claims 1 and 12. By failing to specifically identify those features within Kirsch being relied upon in the rejection, the Examiner has essentially forced Appellants to engage in mind reading and/or guessing to determine how the Examiner is interpreting the elements of the claims and what specific features within Kirsch and Bandini the Examiner believes identically disclose the claimed invention.

THE REJECTION OF CLAIMS 10 AND 11 UNDER 35 U.S.C. § 103

For convenience of the Honorable Board in addressing the rejections, claim 11 stands or falls together with claim 10.

Like claim 1 and 12, claim 10 requires the selection of a message transfer policy based upon a classification of a source of a message. Claim 10 specifically provides:

> 10. A system for classifying electronic mail message transfer requests for policy enforcement comprising:
>
> a mail server;
>
> a set of mail transfer policies, each policy having an association with a corresponding source classification;
>
> at least one table of source identities having a particular classification; and,

> a classifier coupled to said mail server and said at least one table, the classifier identifying a source of an incoming electronic message in the mail server, classifying said source with a classification in the at least one table, **selecting one of the mail transfer policies** based upon the classification, and applying the selected one of the mail transfer policies to said incoming electronic message.

For the reasons set forth in connection with claims 1 and 12, Examiner's failure to provide a claim construction for the term "mail transfer policies" and the resulting failure to apply patentable weight to the claimed element "mail transfer policies" is clear reversible error on the part of the Examiner.

Disappointingly, Appellants provided a clear explanation of Examiner's failure to account for the term "mail transfer policies". Examiner in the Final Office Action, however, chose to ignore Appellants' arguments and instead merely stated, "Applicant's arguments with respect to claims 1-20 have been considered but are moot in view of the new ground(s) of rejection." A clear comparison of page 3 of the Non-Final Office Action dated October 26, 2007 and page 2 of the Final Office Action, however, shows that Examiner did not change one word in the Final Office Action from the Non-Final Office Action in providing a rationale for rejecting claims 1 and 12. Similarly, the Examiner simply has "cut and paste" the identical rejection of claim 10 from the Non-Final Office Action into the Final Office Action. Yet, the Examiner claims to have set forth a "new" ground of rejection. Examiner's behavior in this regard is unacceptable and borders dishonesty.

Based upon the foregoing, Appellants respectfully submit that Examiner neither has properly construed the individual element "message transfer policy" of Appellants' claims, nor has Examiner both identified the requisite corresponding elements of Kirsch relating to such limitations disclosed in the prior art references, and also compared these allegedly corresponding

elements to the individual elements of Appellants' claims 1, 10 and 12. As a result, Appellants believe that the Examiner's rejections under 35 U.S.C. § 103(a) are not viable. Appellants therefore, respectfully solicit the Honorable Board to reverse the Examiner's rejections under 35 U.S.C. § 103(a).

Date: September 17, 2008

Respectfully submitted,

/Steven M. Greenberg/
Steven M. Greenberg
Registration No. 44,725
Customer Number 46321

VIII. CLAIMS APPENDIX

1. (Previously Amended) A method for classifying electronic mail message transfer requests for policy enforcement comprising the steps of:

identifying a source of an incoming electronic message;

classifying said source;

selecting a message transfer policy based upon the classification; and,

applying the selected message transfer policy to said incoming electronic message.

2. (Original) The method of claim 1, wherein said identifying step comprises the step of identifying a network address for said source.

3. (Original) The method of claim 1, wherein said classifying step comprises the step of classifying said source as one of a trusted source, a blocked source, and a suspect source.

4. (Previously Amended) The method of claim 1, wherein said classifying step comprises the step of classifying said source as one of an authenticated source-and an anonymous source.

5. (Original) The method of claim 3, wherein said classifying step further comprises the step of classifying said source as a blocked source where said source appears in a realtime black hole list.

6. (Original) The method of claim 3, wherein said classifying step further comprises the step of classifying said source as a suspect source where said source appears in a realtime black

hole list.

7. (Original) The method of claim 4, wherein said classifying step further comprises the step of classifying said source as an authenticated source only where an authenticated connection has been established with said source.

8. (Original) The method of claim 3, wherein said applying step comprises the step of limiting transfer of messages from a source classified as suspect.

9. (Original) The method of claim 4, wherein said applying step comprises the step of limiting transfer of messages from a source classified as anonymous.

10. (Previously Amended) A system for classifying electronic mail message transfer requests for policy enforcement comprising:

a mail server;

a set of mail transfer policies, each policy having an association with a corresponding source classification;

at least one table of source identities having a particular classification; and,

a classifier coupled to said mail server and said at least one table, the classifier identifying a source of an incoming electronic message in the mail server, classifying said source with a classification in the at least one table, selecting one of the mail transfer policies based upon the classification, and applying the selected one of the mail transfer policies to said incoming electronic message.

11. (Original) The system of claim 10, wherein said at least one table comprises at least one table selected from the group consisting of a table of trusted sources, a table of authenticated sources, a table of suspect sources, a table of blocked sources, and a realtime black hole list.

12. (Previously Amended) A machine readable storage having stored thereon a computer program for classifying electronic mail message transfer requests for policy enforcement, the computer program comprising a routine set of instructions which when executed by a machine cause the machine to perform the steps of:

identifying a source of an incoming electronic message;

classifying said source;

selecting a message transfer policy based upon the classification; and,

applying the selected message transfer policy to said incoming electronic message.

13. (Original) The machine readable storage of claim 12, wherein said identifying step comprises the step of identifying a network address for said source.

14. (Original) The machine readable storage of claim 12, wherein said classifying step comprises the step of classifying said source as one of a trusted source, a blocked source, and a suspect source.

15. (Previously Amended) The machine readable storage of claim 12, wherein said classifying step comprises the step of classifying said source as one of an authenticated source and an anonymous source.

16. (Original) The machine readable storage of claim 14, wherein said classifying step further comprises the step of classifying said source as a blocked source where said source appears in a realtime black hole list.

17. (Original) The machine readable storage of claim 14, wherein said classifying step further comprises the step of classifying said source as a suspect source where said source appears in a realtime black hole list.

18. (Original) The machine readable storage of claim 15, wherein said classifying step further comprises the step of classifying said source as an authenticated source only where an authenticated connection has been established with said source.

19. (Original) The machine readable storage of claim 14, wherein said applying step comprises the step of limiting transfer of messages from a source classified as suspect.

20. (Original) The machine readable storage of claim 15, wherein said applying step comprises the step of limiting transfer of messages from a source classified as anonymous..

IX. EVIDENCE APPENDIX

No evidence submitted pursuant to 37 C.F.R. §§ 1.130, 1.131, or 1.132 of this title or of any other evidence entered by the Examiner has been relied upon by Appellant in this Appeal, and thus no evidence is attached hereto.

X. RELATED PROCEEDINGS APPENDIX

Since Appellant is unaware of any related appeals and interferences, no decision rendered by a court or the Board is attached hereto.